AMENDMENTS TO THE CLAIMS

1-13. **(Canceled)**

14. **(New)** A license information management apparatus which manages license information that includes (i) an encrypted content key for decrypting encrypted digital content and (ii) content reproduction condition information indicating a range in which the digital content can be used, said apparatus comprising:

a storage unit not having tamper resistance, the storage unit being configured to store encrypted information; and

a tamper resistance module which encrypts at least the license information, among the license information and a correspondence table for managing an update history of the license information, and which stores the encrypted information into the storage unit,

wherein the tamper resistance module includes:

a digital signature management unit configured to (i) generate a hash value of the encrypted information before the encrypted information is stored into the storage unit, and hold the generated hash value, and (ii) verify validity of the encrypted information by reading the encrypted information stored in the storage unit, generating a hash value of the read encrypted information, and comparing the generated hash value of the encrypted information before the encrypted information is stored into the storage unit with the generated hash value of the read encrypted information, the validity indicating that the encrypted information has not been tampered with;

an encrypting and decrypting unit configured to (i) encrypt the license information and store the encrypted license information in the storage unit, and (ii) read the encrypted license information from the storage unit and decrypt the read encrypted license information; and

a control unit configured to decrypt the encrypted content key included in the license information decrypted by the encrypting and decrypting unit, output the decrypted content key outside of the license information management apparatus, update the content reproduction condition information included in the decrypted license information, and cause the encrypting and decrypting unit to encrypt the updated license information and to overwrite and store the encrypted updated license information into the storage unit, when the digital content is used and only when the digital signature management unit verifies the validity.

15. **(New)** The license information management apparatus according to Claim 14,

wherein the license information further includes a digital signature for (i) the encrypted content key and (ii) the content reproduction condition information,

wherein the encrypting and decrypting unit is configured to encrypt each of a plurality of pieces of license information, and store each piece of encrypted license information in the storage unit, and

wherein the digital signature management unit is configured to, for a set of all the pieces of encrypted license information, (i) generate a hash value of the digital signature included in the encrypted license information before the encrypted license information is stored into the storage unit, and hold the generated hash value, and (ii) verify the validity of the encrypted license

information by reading the encrypted license information stored in the storage unit, generating a hash value of the digital signature included in the read encrypted license information, and comparing the generated hash value of the digital signature included in the encrypted license information before the encrypted license information is stored into the storage unit with the generated hash value of the digital signature included in the read encrypted license information, the validity indicating that the encrypted license information has not been tampered with.

16. **(New)** The license information management apparatus according to Claim 14,

wherein the encrypting and decrypting unit is further configured to (i) encrypt the correspondence table and store the encrypted correspondence table in the storage unit, and (ii) read the stored correspondence table from the storage unit and decrypt the read correspondence table, the correspondence table being a table in which identification information identifying the license information is stored in association with information indicating an update history of the license information for each of a plurality of pieces of license information stored in the storage unit, and

wherein the digital signature management unit is configured to (i) generate a hash value of the encrypted correspondence table before the encrypted correspondence table is stored into the storage unit, and hold the generated hash value, and (ii) verify validity of the encrypted correspondence table by reading the encrypted correspondence table stored in the storage unit, generating a hash value of the read encrypted correspondence table, and comparing the generated hash value of the encrypted correspondence table before the encrypted correspondence table is

stored into the storage unit with the generated hash value of the read encrypted correspondence table, the validity indicating that the encrypted correspondence table has not been tampered with.

17. **(New)** The license information management apparatus according to Claim 16,

wherein corresponding information indicating the update history indicates the number of updates or a random number, the corresponding information being included in the correspondence table decrypted by the encrypting and decrypting unit, and

wherein the control unit is further configured to update the corresponding information of the correspondence table indicating the number of updates or the random number, when the license information is updated, and cause the encrypting and decrypting unit to encrypt the updated correspondence table and to overwrite and store the encrypted updated correspondence table into the storage unit.

18. **(New)** The license information management apparatus according to Claim 14,

wherein the control unit is further configured to determine whether or not the license information is new, and cause the encrypting and decrypting unit to encrypt the license information, which is determined to be new, and to overwrite and store the encrypted license information into the storage unit.

19. **(New)** The license information management apparatus according to Claim 14,

wherein the tamper resistance module includes an IC card, and

wherein the storage unit includes a flash memory.

20. **(New)** A license information management method for managing, by using a tamper resistance module, license information that includes (i) an encrypted content key for decrypting encrypted digital content and (ii) content reproduction condition information indicating a range in which the digital content can be used, the tamper resistance module being capable of writing and reading encrypted information to a storage unit storing the encrypted information and having no tamper resistance, encrypting at least the license information, among the license information and a correspondence table for managing an update history of the license information, and storing the encrypted license information into the storage unit, said method comprising:

a digital signature management step of (i) generating and holding a hash value of the encrypted information before the encrypted information is stored into the storage unit, and (ii) verifying validity of the encrypted information by reading the encrypted information stored in the storage unit, generating a hash value of the read encrypted information, and comparing the generated hash value of the encrypted information before the encrypted information is stored into the storage unit with the generated hash value of the read encrypted information, the validity indicating that the encrypted information has not been tampered with;

an encrypting and decrypting step of (i) encrypting the license information and storing the encrypted license information in the storage unit, and (ii) reading the encrypted license information from the storage unit and decrypting the read encrypted license information; and

a control step of decrypting the encrypted content key included in the license information

decrypted in the encrypting and decrypting step, outputting the decrypted content key outside a license information management apparatus, updating the content reproduction condition information included in the decrypted license information, and causing the updated license information to be encrypted in the encrypting and decrypting step and to be overwritten and stored into the storage unit.

21. **(New)** A computer executable program embodied on a computer-readable medium, the program being for use in a license information management apparatus which manages, by using a tamper resistance module, license information that includes (i) an encrypted content key for decrypting encrypted digital content and (ii) content reproduction condition information indicating a range in which the digital content can be used, the tamper resistance module being capable of writing and reading encrypted information to a storage unit storing the encrypted information and having no tamper resistance, encrypting at least the license information, among the license information and a correspondence table for managing an update history of the license information, and storing the encrypted license information into the storage unit, said program causing a computer to execute a method comprising:

a digital signature management step of (i) generating and holding a hash value of the encrypted information before the encrypted information is stored into the storage unit and (ii) verifying validity of the encrypted information by reading the encrypted information stored in the storage unit, generating a hash value of the read encrypted information, and comparing the generated hash value of the encrypted information before the encrypted information is stored into

the storage unit with the generated hash value of the read encrypted information, the validity indicating that the encrypted information has not been tampered with;

an encrypting and decrypting step of (i) encrypting the license information and storing the encrypted license information in the storage unit, and (ii) reading the encrypted license information from the storage unit and decrypting the read encrypted license information; and

a control step of decrypting the encrypted content key included in the license information decrypted in the encrypting and decrypting step, outputting the decrypted content key outside the license information management apparatus, updating the content reproduction condition information included in the decrypted license information, and causing the updated license information to be encrypted in the encrypting and decrypting step and to be overwritten and stored into the storage unit.